UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,390	03/25/2004	Masaharu Ukeda	520.43700X00	5523

20457 7590 03/20/2008

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/808,390	**Applicant(s)** UKEDA ET AL.	
	Examiner TECHANE J. GERGISO	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 07/15//2004.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 03/25/2004.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the applicant's communication filed on July 15, 2004.

2. Claims 1-16 have been examined and are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishino et al. (US Pat. No.: 5,857,024) in view of Tan et al. (US Pub. No.: 2001/0045451).

As per claim 1:

Nishino discloses an individually usable memory device, connectable to a host device, for performing mutual authentication between a server device and the memory device by use of a passcode, comprising

an interface adapted to receive time information from said host device (column 3: lines 17-45; Figure 1: 32; I/O);

a non-volatile memory for storing pass-information (column 3: lines 20-45; Figure 1: 30; 38); and a processing device which, in response to a request from said host device, generates said passcode from the pass-information in said non-volatile memory and a time information from said host device, and which transmits said passcode to said host device through said interface without sending said pass-information to said host device (column 5: lines 40-63; figure 3: 202-210).

Nishino does not explicitly teach performing mutual authentication between a server device and the memory device and pass-information related said server device. Tan et al., in an analogous art, teaches teach performing mutual authentication between a server device and the memory device and pass-information related said server device (*0008; 0021; the cardholder 12 authenticates himself or herself to the smart card 10 using the cardholder's PIN, the card 10 establishes a mutual authentication with an access server 14 using SSL protocol authentication*). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Nishino to include performing mutual authentication between a server device and the memory device and pass-information related said server device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide token based user access authentication that enables secure user access to a web server using, for example, a smart card and the token based user access authentication makes use of the token authentication process of the single sign-on mechanism, but does not employ a user name and password in the log on process as suggested by Tan et al. (in 0006-0008).

As per claim 2

Nishino discloses the memory device, wherein the memory device is configured such that a success-time of the mutual authentication between said memory device and said server device via said host device is stored in said non-volatile memory, so that it is impossible to illegally alter the stored success-time afterwards, and whether or not the memory device may be used is controlled on the basis of said success-time that cannot be illegally altered (column 2: lines 50-65; a clock for counting time. Figure 4: 222-2228).

As per claim 3:

Nishino discloses the memory device, wherein:

said processing device includes a time examination unit for verifying the time information from said host device (Figure 4: 222-2228; column 7: lines 25-40);

said time examination unit stores the time information when an initial time verification is successful (Figure 4: 222-2228; column 7: lines 25-40); and

said processing device causes generation of said passcode to be failed when the time information from said host device is not later than the success time of said connection authentication, and causes generation of said passcode to be failed or said passcode to be deleted when the time information from said host device is later than an expiration date of said pass-information, so that the passcode to be transmitted to said host device may be limited to the predetermined number of bytes (Figure 4: 222-2228; column 7: lines 25-40; Figure 5:222-230; Column 7: lines 56-66).

As per claim 4:

Tan discloses the memory device, wherein: said processing device encrypts license data that can be used for protection of a copy right after the mutual authentication with either said host device or said server device, stores the license date in said non-volatile memory, stores said pass-information in said non-volatile memory as license data, and with reading-out of the license data being prohibited afterwards, makes it possible to use the license data for the generation of said passcode (Figure 4: authentication; Certificate).

As per claim 5:

Tan discloses the memory device, wherein: said non-volatile memory holds license data with an expiration date; and said processing device compares the expiration date of said license data with said success-time when said license data is accessed, and stops the access to the license data with said expiration date or delete said license data when the expiration date is not later than said success time (Figure 4: authentication; Certificate).

As per claim 6:

Nishino discloses a single chip microcomputer that is mounted on an individually usable memory device, connectable to a host device, comprising:

receiving means adapted for receiving a time information from said host device (column 3: lines 17-45; Figure 1: 32; I/O);

reading-out means for reading out from a non-volatile memory in said memory device a pass-information (column 3: lines 20-45; Figure 1: 30; 38);

generating means for generating said passcode on the basis of said pass-information and time information from said host device (column 5: lines 40-63; Figure 3: 208); and

transmittance means for transmitting said passcode to said host device through an interface within said memory device without transmitting said pass-information to said host device (column 5: lines 40-63; Figure 3: 210).

Nishino does not explicitly teach performing mutual authentication between a server device and the memory device and pass-information related said server device defined for each user for said memory device. Tan et al., in an analogous art, teaches teach performing mutual authentication between a server device and the memory device and pass-information related said server device defined for each user for said memory device (*0008; 0021; the cardholder 12 authenticates himself or herself to the smart card 10 using the cardholder's PIN, the card 10 establishes a mutual authentication with an access server 14 using SSL protocol authentication*). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Nishino to include performing mutual authentication between a server device and the memory device and pass-information related said server device defined for each user for said memory device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide token based user access authentication that enables secure user access to a web server using, for example, a smart card and the token based user access authentication makes use of the token authentication process of the single sign-on mechanism, but does not employ a user name and password in the log on process as suggested by Tan et al. (in 0006-0008).

As per claim 7:

Nishino discloses the memory device, wherein a success-time of the mutual authentication between said memory device and said server device via said host device is written into said non-volatile memory, said memory device is configured such that said success-time stored cannot be illegally altered afterwards, and whether or not the memory device can be used is controlled on the basis of said success-time that cannot be illegally altered (column 2: lines 50-65; a clock for counting time. Figure 4: 222-2228).

As per claim 8:

Nishino discloses a passcode generator, connectable to a first computer used by a user, comprising:

an interface connected to said first computer (column 3: lines 17-45; Figure 1: 32; I/O);

a memory for storing pass-information agreeing with pass-information stored in computer and a user ID of said user (column 3: lines 20-45; Figure 1: 30; 40);

a time examination unit for, time information being stored therein or in said memory, comparing time information from said first computer with the time information stored therein or in said memory when receiving the time information from said first computer, and updating the time information stored therein or in said memory to the time information from said first computer when the time information from said first computer is later than the time information stored therein or in said memory (column 5: lines 40-63; Figure 1: 42; Figure 4: 222-228; Figure 5: 222-230); and

a random number generator for generating said passcode on the basis of the pass-information in said memory and the time information stored therein or in said memory, and sending said passcode and said user ID to said first computer through said interface when the time information from said first computer is later than the time information stored therein or in said memory (Column 5: 45-65).

Nishino does not explicitly teach performing mutual authentication between a second computer and the memory device and pass-information related said a second computer defined for each user for said memory device. Tan et al., in an analogous art, teaches teach performing mutual authentication between a second computer and the memory device and pass-information related said second computer defined for each user for said memory device (*0008; 0021; the cardholder 12 authenticates himself or herself to the smart card 10 using the cardholder's PIN, the card 10 establishes a mutual authentication with an access server 14 using SSL protocol authentication*). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Nishino to include performing mutual authentication between a second computer and the memory device and pass-information related said second computer defined for each user for said memory device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide token based user access authentication that enables secure user access to a web server using, for example, a smart card and the token based user access authentication makes use of the token authentication process of the single sign-on mechanism, but does not employ a user name and password in the log on process as suggested by Tan et al. (in 0006-0008).

As per claim 9:

Nishino discloses a passcode generator, wherein said random number generator sends error information in place of said passcode to said first computer through said interface when the time information from said first computer is not later than the time information stored therein or in said memory (Column 5: 45-65; column 2: lines 50-65; a clock for counting time. Figure 4: 222-2228).

As per claim 10:

Nishino discloses a passcode generator, wherein said memory stores a password; and

said time examination unit, when the time information from said first computer is not later than the time information stored therein or in said memory, compares the password from said first computer with the password in said memory, and if the password from said first computer agrees with the password in said memory, updates the time information stored therein or in said memory to the time information from said first computer (Column 5: 45-65; column 2: lines 50-65; a clock for counting time. Figure 4: 222-2228; Figure 5: 222-230).

As per claim 11:

Nishino discloses a passcode generator, wherein said memory stores data with an expiration date therein; and said passcode generator includes a data supervising unit for verifying said expiration date using the time information stored therein or in said memory which were updated, when the time information from said first computer is later than the time information in said memory (Column 5: 45-65; Figure 1: 40; 36; 42; Figure 4: 222-2228; Figure 5: 222-230).

As per claim 12:

Nishino discloses a passcode generator, wherein,

said memory stores encrypted content data therein (Figure 1: 36, 40; Column 5: 45-65);

said data with an expiration date is a license for decrypting said content data (Figure 3: 204; 208; Column 5: 45-65); and

said data supervising unit receives said data with an expiration date sent from said second computer through said first computer and said interface when said second computer is successful in user authentication using said passcode and stores said received data with an expiration date (Column 5: 45-65; Figure 1: 40; 36; 42; Figure 4: 222-2228; Figure 5: 222-230).

As per claim 13:

Nishino discloses a passcode generator, wherein

said memory stores a password therein; said data supervising unit makes said data with an expiration date invalid when the time information from said first computer is not later than the time information stored therein or in said memory, and makes said invalidated data with an expiration date valid when the password from said first computer is compared with the password in said memory and the password from said first computer agrees with the password in said memory (Column 5: 45-65; Figure 1: 40; 36; 42; Figure 4: 222-2228; Figure 5: 222-230).

As per claim 14:

Tan et al. discloses a passcode generator, wherein said password is a password given to a administrator different from said user (0026).

As per claim 15:

Nishino discloses a passcode generator, wherein

said time examination unit stores the number of updates of time information stored therein or in said memory and sends error information in place of said passcode to said first computer through said interface when said number of updates exceeds a predetermined number of update times within a predetermined period of time (Column 5: 45-65; Figure 1: 40; 36; 42; Figure 4: 222-2228; Figure 5: 222-230).

As per claim 16:

Nishino discloses a passcode generator, connectable to a first computer used by a user, which generates a passcode for authenticating the user with a second computer capable of communicating with said first computer, comprising:

an interface connected to said first computer (column 3: lines 17-45; Figure 1: 32; I/O);

a memory for storing pass-information agreeing with the pass-information stored in said second computer and a user ID of said user (column 3: lines 20-45; Figure 1: 30; 40);

a time examination unit for, time information stored therein or in said memory, sending the time information stored therein or in said memory to said first computer, receiving the time information in said first computer from said first computer when said first computer judges that the time information in said first computer is later than the time information stored therein or in said memory, and updating the time information stored therein or in said memory to the time information from said first computer (column 5: lines 40-63; Figure 1: 42; Figure 4: 222-228; Figure 5: 222-230); and

a random number generator for generating said passcode on the basis of the pass-information in said memory and said time information and sending said passcode and said user ID to said first computer through said interface when the time information in said first computer is later than the time information stored therein or in said memory (Column 5: 45-65).

Nishino does not explicitly teach performing mutual authentication between a second computer and the memory device and pass-information related said a second computer defined for each user for said memory device. Tan et al., in an analogous art, teaches teach performing mutual authentication between a second computer and the memory device and pass-information related said second computer defined for each user for said memory device (*0008; 0021; the cardholder 12 authenticates himself or herself to the smart card 10 using the cardholder's PIN, the card 10 establishes a mutual authentication with an access server 14 using SSL protocol authentication*). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Nishino to include performing mutual authentication between a second computer and the memory device and pass-information related said second computer defined for each user for said memory device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide token based user access authentication that enables secure user access to a web server using, for example, a smart card and the token based user access authentication makes use of the token authentication process of the single sign-on mechanism, but does not employ a user name and password in the log on process as suggested by Tan et al. (in 0006-0008).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art

Contact Information

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137